

Date: 2/2/00

FORM PTO-1449

INFORMATION DISCLOSURE CITATION

Atty Docket

Serial No.

162/547

To be assigned

Applicant

Shiho Moriai et al.

Filing Date

Herewith

Group Art Unit

To be assigned

U.S. PATENT DOCUMENTS

Examiner Initial		Document Number	Date	Name	Class	Sub-Class	Filing Date
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						

FOREIGN PATENT DOCUMENTS

		Document Number	Date	Country	Class	Sub-Class	Translation
	AL						Yes No
	AM						Yes No

OTHER (Including Author, Title, Date, Pertinent Pages, etc.)

	AN		Shiho Moriai, "How to Design Secure S-boxes against Differential, Linear, Higher Order Differential, and Interpolation Attacks," Telecommunications Advancement Organization of Japan, SCIS '98, 2.2C, January 1998, pp. 1-8
	AO		Hamade, Takeshi, et al., "On Partitioning Cryptanalysis of DES," Telecommunications Advancement Organization of Japan, SCIS '98, 2.2A, January 1998, pp. 1-8
	AP		Langford, S.K., and Hellman, M.E., "Differential-Linear Cryptanalysis," <u>Lecture Notes in Computer Science</u> , Advances in Cryptology CRYPTO '94, Vol. 839, 1994, pp. 17-25
	AQ		Sakurai, Kouichi, "Angou riron no kiso," Kyoritsu Shuppan, pp. 69-72, 1996
	AR		Kanda, Masayuki, et al., "A Round Function Structure Consisting of Few S-boxes (Part II)," Telecommunications Advancement Organization of Japan, SCIS '98, 2.2.D, January 1998, pp. 1-8
	AS		Moriai, Shiho, et al., "S-box Design Considering the Security Against Known Attacks on Block Ciphers," Technical Report of the IEICE, ISEC98-13, Vol. 98, NO. 227, 30 July 1998, pp. 25-32

Examiner

Date Considered

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP § 609.

Draw line through citation if not in conformance and not considered.

Include copy of this form with next communication to Applicant.